UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,722	03/24/1999	DAVID A. LEE	042390.P6526	1130

7590 03/11/2004

WILLIAM W SCHAAL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
HAMILTON, MONPLAISIR G	
ART UNIT	**PAPER NUMBER**
2172	6

DATE MAILED: 03/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/275,722	LEE, DAVID A.	
	Examiner	Art Unit	
	Monplaisir G Hamilton	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 remain for examination.

Drawings

2. The drawings were received on 12/1/03. These drawings are acceptable.

Response to Arguments

3. Applicant's arguments, see Paper No 5 Section 2, filed 12/1/03, with respect to Claims 1-19 and 23-27 have been fully considered and are persuasive. The 35 U.S.C. § 101 rejections of Claims 1-19 has been withdrawn.

4. Applicant's arguments filed 12/1/03, Paper No. 5, have been fully considered but they are not persuasive.

Applicant argues: "[t]he PTO has also rejected claims 1-4, 11-14 and 20 under 35 U.S.C. § 103(a) based upon Lotspiech in combination with Luther. The rejection of these claims is respectfully traversed. Applicant respectfully asserts that the combination set forth by the PTO fails to meet the requirement for a prima facie case for a § 103(a) rejection for at least the following reasons.

It is respectfully asserted that neither Lotspiech nor Luther, either alone or in combination, suggests or describes ***using a matrix of keys to produce a first set of secret device keys that are in turn used to produce a shared secret key***. The PTO asserts that Lotspiech discloses a matrix of device keys producing a "shared secret key." The PTO does not assert that Luther provides the necessary middle step. Therefore, even if the combination were proper, although Applicants believe that it is not, nonetheless, the combination would still fail to produce the

invention as recited in the rejected claims. It is, therefore, respectfully requested that the rejection of this claim be withdrawn."

Examiner disagrees with applicant. Lotspiech discloses providing each device with plural device keys (col 5, lines 9-15, Fig 3). Lotspiech further discloses that a session key block is generated based upon an encryption operation between the device keys and N session numbers (col 5, lines 45-68; Fig. 4). The session block is the used to generate a common/shared key (col 6, lines 30-42). The claimed secret device keys is equivalent to disclosed device keys. Additionally, the common key disclosed by Lotspiech is equivalent to claimed shared key. Examiner maintains that the claimed invention is unpatentable.

Applicant further argues: "Claims 2-4, 11-14 and 20 either depend from and include the limitations of claim 1, or include a substantially similar and patentably distinct limitation as claim 1. Therefore, these claims patentably distinguish from the cited patents on the same basis as claim 1. It is, therefore, respectfully requested that the PTO withdraw the rejections of claims 1-4, 11-14 and 20."

Examiner disagrees with applicant's argument. As noted in the rebuttal above, the Lotspiech in view of Luther discloses all the limitations of Claim 1 above. Therefore the previous rejections regarding Claims 2-4, 11-14 and 20 is maintained.

Applicant further argues: "The PTO has noted via form PTO-326 that claims 1-27 are rejected. However, Applicant is unable to determine why claims 21 and 22 are rejected. Applicant respectfully requests clarification regarding these claims. Specifically, are the claims allowed, rejected, or merely objected to as being dependent upon rejected claim 21?"

Because these claims were not addressed in the pervious action, this action is made Non-Final. These claims are addressed below.

Claim Objections

5. Claim 16 is objected to under 37 CFR 1.75 as being a substantial duplicate of Claim 6. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 11-15, 17-27 rejected under 35 U.S.C. 102(e) as anticipated by US 6118873 issued to Lotspiech et al, herein referred to as Lotspiech.

Referring to Claim 11:

Lotspiech discloses a method comprising providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2 (Fig 3; col 5, lines 5-20); for each row of the key matrix, performing arithmetic operations on matrix keys of at least two selected columns of the key matrix to produce a first set of secret device keys (col 5, lines 55-68); producing a shared

secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys (col 6, lines 25-43).

Referring to Claim 13:

Lotspiech discloses the limitations as discussed in Claim 11 above. Lotspiech further discloses prior to performing the arithmetic operations, the method comprises: generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys (col 5, lines 55-68).

Referring to Claim 14:

Lotspiech discloses the limitations as discussed in Claim 11 above. Lotspiech further discloses the key selection vector is uniquely assigned to a first digital platform (col 5, lines 60-65).

Referring to Claim 15:

Lotspiech discloses the limitations as discussed in Claim 14 above. Lotspiech further discloses wherein prior to producing the shared secret key, the method comprises: receiving a key selection vector from a second digital platform in communication with the first digital platform (col 5, lines 40-50); and analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys (col 5, lines 10-30, 40-65).

Referring to Claim 17:

Lotspiech discloses the limitations as discussed in Claim 11 above. Lotspiech further discloses producing of the shared secret key comprises: analyzing contents of an incoming key selection vector (col 6, lines 30-35); and performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector (col 6, lines 35-40).

Referring to Claim 18:

Lotspiech discloses the limitations as discussed in Claim 17 above. Lotspiech further discloses the producing of the shared secret key further comprises: performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector (col 6, lines 34-40).

Referring to Claim 19:

Lotspiech discloses a machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising: an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector (col 6, lines 10-42); a transfer function to output at least a key selection vector assigned to the first digital platform (col 6, lines 30-40); a hash function to perform a hash operation on at least the shared secret key to produce a

resultant hash value (col 6, lines 30-40); and a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector (col 6, lines 30-40; col 6, lines 20-30).

Referring to Claim 20:

Lotspiech discloses a network comprising: a first digital platform; and a certification authority in communication with the first digital platform (Fig 1; col 5, lines 5-20), the certification authority having access to a key matrix featuring matrix keys arranged in accordance with at least a first dimension and a second dimension (col 5, lines 30-50), generating a first key selection vector and providing a first set of secret device keys produced from selected matrix keys of the key matrix (col 5, lines 40-50).

Referring to Claim 21:

Lotspiech discloses the limitations of Claim 20 above. Lotspiech further discloses a second digital platform in communication with the certification authority and the first digital platform (col 6, lines 55-68; col 8, lines 30-40), the second digital platform being uniquely assigned a second key selection vector indicating at least two grids of the key matrix (col 6, line 60-col 7, line 10) and a second set of secret device keys produced from matrix keys situated in at least two grids of the key matrix (col 7, lines 10-25).

Referring to Claim 22:

Lotspiech discloses the limitations of Claim 21 above. Lotspiech further discloses the first and second digital platforms to exchange the first and second key selection vectors in order for each digital platform to produce a shared secret key to ensure that communications between the first and second digital platforms are secure (col 8, lines 30-45).

Referring to Claim 23:

Lotspiech discloses a certification authority comprising: a memory to store a key matrix having N rows and M columns of matrix keys, where N>_2 and M>_2 (Fig 1; Fig 3; col 5, lines 10-20); a logic to generate a key selection vector for each digital platform registered with the certification authority (col 5, lines 20-30, 40-50).

Referring to Claim 24:

Lotspiech discloses the limitations of Claim 23 above. Lotspiech further discloses the logic includes a processing unit (col 4, lines 5-20).

Referring to Claim 25:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the processing unit produces a first set of secret device keys by performing arithmetic operations on matrix keys along selected columns of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform (col 5, lines 50-68).

Referring to Claim 26:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the matrix keys along the processing unit performs arithmetic operations on matrix keys along selected rows of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform (col 6, lines 30-45).

Referring to Claim 27:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the matrix keys are only known by the certification authority (col 5, lines 15-20).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, 9-10, 12 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6118873 issued to Lotspiech et al, herein referred to as Lotspiech in view of US 5533127 issued to Luther, herein referred to as Luther.

Referring to Claim 1:

Lotspiech discloses a method comprising: providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2 (Fig 3; col 5, lines 5-20); for each column of the key matrix performing arithmetic operations on matrix keys [~~of at least two selected rows of the key matrix to produce a first set of secret device keys~~]" (col 6, lines 30-40); producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys (col 6, lines 25-42).

Lotspiech does not explicitly disclose "[~~for each column of the key matrix~~], performing arithmetic operations on matrix keys of at least two selected rows of the key matrix to produce a first set of secret device keys.

Luther discloses performing arithmetic operations on matrix key of least two selected rows of the key matrix to produce a first set of secret device keys (col 3, lines 15-35; Fig 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that arithmetic operations on matrix keys of at least two selected rows of the key matrix to produce a first set of secret device keys. One of ordinary skill in the art would have been motivated to do this because it would provide a method for generating a common key (Lotspiech: col 6, lines 35-42).

Referring to Claim 2:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 1 above. Luther further discloses the arithmetic operations include modular addition (col 7, lines 35-50; Fig .9).

Referring to Claim 3:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses prior to performing the arithmetic operations, the method comprises: generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys (col 5, lines 55-68).

Referring to Claim 4:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 3 above. Lotspiech further discloses the key selection vector is uniquely assigned to a first digital platform (col 5, lines 60-65).

Referring to Claim 5:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 4 above. Lotspiech further discloses wherein prior to producing the shared secret key, the method comprises: receiving a key selection vector from a second digital platform in communication with the first digital platform (col 5, lines 40-50); and analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys (col 5, lines 10-30, 40-65).

Referring to Claims 6 and 16:

Lotspiech in view of Luther discloses the limitations as discussed in Claims 1 and 11 above. Lotspiech further discloses prior to performing arithmetic operations on keys of at least two selected rows, the method further comprises: dedicating the rows of the key matrix to a first classification (col 5, lines 30-40; Fig. 3; sets); and dedicating the columns of the key matrix to a second classification (col 5, lines 30-40; Fig. 3; index).

Referring to Claim 7:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 6 above. Lotspiech further discloses first classification includes digital platforms designed to provide information to other digital platforms (col 4, lines 45-65).

Referring to Claim 8:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 7 above. Lotspiech further discloses the second classification includes digital platforms designed to receive information from other digital platforms (col 4, lines 45-65).

Referring to Claim 9:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 1 above. Lotspiech further discloses producing of the shared secret key comprises: analyzing contents of an incoming key selection vector (col 6, lines 30-35); and performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector (col 6, lines 35-40).

Referring to Claim 10:

Lotspiech in view of Luther discloses the limitations as discussed in Claim 9 above. Lotspiech further discloses the producing of the shared secret key further comprises: performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector (col 6, lines 34-40).

Referring to Claim 12:

Lotspiech discloses the limitations as discussed in Claim 11 above.

Lotspiech does not explicitly disclose "the arithmetic operations include modular addition."

Luther further discloses the arithmetic operations include modular addition (col 7, lines 35-50; Fig .9).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that arithmetic operation is modular addition. One of ordinary skill in the art would have been motivated to do this because it would provide a method for generating a common key (Lotspiech: col 6, lines 35-42).

Prior Art

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 5860136 issued to Fenner, Peter R. Fenner discloses to provide fast access times with very large key fields, an associative memory utilizes a location addressable memory and lookup table to generate from a key the address in memory storing an associated record. The lookup tables, stored in memory, are constructed with the aid of arithmetic data compression methods to create a near perfect hashing of the keys. For encoding into the lookup table, keys are divided into a string of symbols. Each valid and invalid symbol is assigned an index value, such that the sum of valid index values for symbols of a particular key is a unique value that is used as an address to the memory storing the record associated with that key, and the sum of

keys containing invalid index values point to a location in memory containing similar data. Utilizing the lookup tables set and relational operations maybe carried out that provide a user with a maximum number of key records resulting from a sequence of intersection, union and mask operations.

US 5708714 issued to Lopez, Jose Manuel Cerecedo et al. Lopez discloses the object of the present invention is to perform verifiable secret sharing by a practical amount of calculation and a practical amount of communication. In addition, by using this process, a shared digital signature is generated, or a shared authentication server is provided.

In a communication system where a plurality of information processing apparatuses are connected across secret communication channels and a broadcast communication channel, an information processing apparatus d generates a secret matrix from secret information s, l1, . . . , lk, extracts the first information segments for individual apparatuses i, and secretly transmits it to each apparatus i. The information processing apparatus d performs hash function on the secret matrix and broadcasts the output value. Each information processing apparatus i generates and broadcasts a random number, while the information processing apparatus d generates and broadcasts the second information segment from a partial array in consonance with the random number value. Each information processing apparatus i generates the third information segment in consonance with the first information segment and the random number, and verifies that the secret information has been correctly shared by comparing the third information segment with the second. By employing this secret information sharing method,

apparatuses that belong to a group of signers cooperatively generate a signature, and a plurality of apparatuses that constitute authentication servers cooperatively provide authentication.

US 5295188 issued to a high-speed public key cryptosystem is constructed for the encryption and decryption of digital data blocks, the creation and verification of digital signatures, and the creation of verifiable random number sequences. The encryption and decryption techniques employ a public key K constructed as the matrix product of a randomly generated nonsingular matrix M, and a rectangular template matrix T having row identifiers imbedded therein for selecting rows of a matrix M-1 that participate during decryption. Encrypting of a plaintext block, is achieved by converting the block to a nonlinear row selector code used to select rows of K. Columns of the selected rows are then added modulo-2 to produce a block if ciphertext. Deciphering the ciphertext is an iterative process wherein successive row identifiers and plaintext bits are unmasked by selecting rows of matrix M-1 in accordance with the bit states of the ciphertext, and adding columns of the selected rows modulo-2 to produce an intermediate block of data containing 2 plaintext bits and a row identifier used to select a row of key T, which is then added modulo-2 to the intermediate block to reveal the next two bits of plaintext and the next row identifier. A public key consisting of a single, noninvertible, binary matrix and a private key consisting of a pair of binary matrices, one or which is singular and the other nonsingular.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monplaisir G Hamilton whose telephone number is (703) 305-5116. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Monplaisir Hamilton

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100